CLAIMS

Therefore, having thus described the invention, at least the following is claimed:

1. A method for providing information on system vulnerabilities, comprising:

populating a database with element or system vulnerability information;

obtaining keywords from profile or policy-descriptive information for the system; and

selecting a database page to access from a database structure configured as a hierarchical plurality of database pages, each database page having a page index, data section and selector section, and utilizing keyword matching between the descriptive information and selector section to obtain vulnerability information for an element or combination of elements.

2. The method of claim 1, further comprising storing intermediate result or status information obtained from the selecting step in a state accumulator module.

3. The method of claim 2, further comprising performing a check of the state accumulator module for intermediate result or status information.

4. The method of claim 3, wherein the selecting step further comprises matching keywords utilizing result or status information stored in the state accumulator module.

5. The method of claim 4, further comprising sending the vulnerability information to a vulnerability accumulator module;

retaining page selector information for database pages accessed; and

updating intermediate result or status information in the state accumulator module.

6. The method of claim 5, further comprising detecting a selection of input from a user, including profile or policy-descriptive system information provided by the user, to continue the obtaining keywords step and selecting step for same element.

7. The method of claim 1, further comprising repeating the obtaining keywords step and selecting step for another element or element combination.

8. The method of claim 1, further comprising updating at least one of an element counter value, combination counter value, cycle counter value, or cumulative cycle counter value.

9. The method of claim 5, further comprising updating the database with an element counter value.

10. The method of claim 9, further comprising updating the database with list of database pages or indices accessed to provide for accumulated vulnerability results for examined element or system.

11. The method of claim 10, further comprising presenting the accumulated vulnerability results to a user's processing device.

12. The method of claim 1, further comprising filtering information on the element or combination of elements prior to performing the obtaining keywords step.

13. The method of claim 2, further comprising identifying and selecting particular combinations of system elements to process based on vulnerability information obtained from the database as well as on state information stored in the state accumulator.

14. A computer-readable medium having a computer program for providing information on system vulnerabilities for performing the steps of:

logic configured to populate a database with element or system vulnerability information;

logic configured to query a database to obtain descriptive information for the system;

logic configured to select a database page to access from a database structure configured as a hierarchical plurality of database pages, each database page having a page index, data section and selector section; and

logic configured to perform keyword matching between the descriptive information and selector section to obtain vulnerability information for an element or combination of elements.

15. The computer-readable medium of claim 14, further comprising logic configured to store intermediate result or status information obtained from the select logic in a state accumulator module.

16. The computer-readable medium of claim 15, further comprising logic configured to perform a check of a state accumulator module for intermediate result or status information.

17. The computer-readable medium of claim 16, wherein the logic configured to select from a database page to access is further configured to match keywords utilizing result or status information stored in the state accumulator module.

18. The computer-readable medium of claim 17, further comprising logic configured to send the vulnerability information to a vulnerability accumulator module;

logic configured to retain page selector information for database pages accessed; and

logic configured to update intermediate result or status information in the state accumulator module.

19. The computer-readable medium of claim 18, further comprising logic configured to detect a selection of input from a user, including profile/policy-descriptive system information provided by the user, to continue the performing of query logic and select logic for same element.

20. The computer-readable medium of claim 14, further comprising logic configured to continue cycling by repeating the performing of query logic and select logic for another element or element combination.

21. The computer-readable medium of claim 14, further comprising logic configured to update at least one of an element counter value, combination counter value, cycle counter value, or cumulative cycle counter value.

22. The computer-readable medium of claim 18, further comprising logic configured to update the database with at least one of an element counter value, combination counter value, cycle counter value, or cumulative cycle counter value.

23. The computer-readable medium of claim 22, further comprising logic configured to update the database with list of database pages or indices accessed to provide for accumulated vulnerability results for examined element or system.

24. The computer-readable medium of claim 23, further comprising logic configured to present the accumulated vulnerability results to a user's processing device.

25. The computer-readable medium of claim 14, further comprising logic configured to filter information on the element or combination of elements prior to performing the query logic.

26. A system for providing information on system vulnerabilities, comprising:

a database populated with descriptive system information;

a database structure configured as a hierarchical plurality of database pages, each database page further comprises a page index, data section and selector section, and wherein the data section is further configured to include the element vulnerability information and the selector section is further configured to include links to related database pages; and

a rule processor module configured to provide rules for cycling through the database structure to match keywords provided by user input, including profile/policy-descriptive system information provided by the user, and the descriptive system information from the database with element vulnerability information from the database structure.

27. The system of claim 26, further comprising an input parser/filter module operatively coupled to the rule processor module, the input parser/filter module configured to receive policy or profile input from a user's processing device and to convert the input into data usable by the rule processor module.

28. The system of claim 26, further comprising a state accumulator module operatively coupled to the rule processor module, the state accumulator module configured to store intermediate vulnerability status or result information.

29. The system of claim 26, further comprising a vulnerability accumulator module operatively coupled to the rule processor module, the vulnerability accumulator module configured to store identified vulnerability result information.

30. The system of claim 26, further comprising a presentation module operatively coupled to a user's processing device and the vulnerability accumulator module, the presentation module configured to summarize and format accumulated vulnerability results for utilization by the user's processing device.

31. The system of claim 26, further comprising a database interface module operatively coupled between the database, database structure, and the result accumulator module, the database interface module configured to enable provisioning and access to the database and the database structure.

32. The system of claim 26, wherein the database comprises an element descriptive database (EDD).

33. The system of claim 26, wherein the database structure comprises a hierarchical vulnerability database (HVD) structure.

34. The system of claim 28, wherein the rules processor module is further configured to utilize accumulated state information from the state accumulator module to modify the matching or filtering of keywords, such that a likelihood of success of a probability of matching or filtering of keywords is changed based upon at least one of probabilistic, statistical, conditional pre-requisite item, occurrence, situation, or rules information.

35. A system for providing system vulnerability information, comprising:

a database populated with descriptive system information;

a database structure configured as hierarchical plurality of database pages, each database page including a page index, data section and selector section, and wherein the data section is further configured to include the element vulnerability information and the selector section is further configured to include links to related database pages;

a rule processor module configured to provide rules for cycling through the database structure to match keywords provided by user input, including profile/policy-descriptive system information provided by the user, and the descriptive system information from the database with element vulnerability information from the database structure;

an input parser/filter module operatively coupled to the rule processor module, the input parser/filter module configured to receive policy or profile input from a user's processing device and to convert the input into data usable by the rule processor module;

a state accumulator module operative coupled to the rule processor module, the state accumulator module configured to store intermediate vulnerability status and result information; and

a vulnerability accumulator module operatively coupled to the rule processor module, the vulnerability accumulator module configured to store identified vulnerability result information.

36. The system of claim 35, further comprising a presentation module operatively coupled to a user's processing device and the vulnerability accumulator module, the presentation module configured to summarize and format accumulated vulnerability results for utilization by the user's processing device.

37. The system of claim 36, further comprising a database interface module operatively coupled between the database and database structure, and the result accumulator module, the database interface module configured to enable provisioning and access to the database and the database structure.

38. The system of claim 37, wherein the database comprises an element descriptive database (EDD).

39. The system of claim 37, wherein the database structure comprises a hierarchical vulnerability database (HVD) structure.